Systèmes UNIX. TDs 7 et 8 : chiffrement

Voici la liste des exercices à faire. Organisez vous en binômes. Les exercices de complexité élevée sont marquées d'un astérisque★. Ils ne sont pas obligatoires. Ils sont conçus spécialement pour les étudiant(e)s motivé(e)s qui peuvent facilement résoudre les exercices sans astérisque.

1 ROT13 — un algorithme simpliste de chiffrement de texte

Alice souhaite envoyer un message crypté à Bob. Après un moment de réflexion, elle a choisi l'algorithme ROT13. Voici donc son message :

```
URYYB OBO, ZL CNERAGF NER ABG NG UBZR, PBZR BIRE GB QEVAX FBZR GRR,
FGHQL HAVK NAQ PELCGBTENCUL.
```

Bob ne sait pas comment le déchiffrer. Il demande votre aide. Vous avez rapidement trouvé un article sur Wikipedia, expliquant son fonctionnement. Voici l'article : https://fr.wikipedia.org/wiki/ROT13

EXERCICE 1.1. Pourriez-vous aider Bob à déchiffrer le message d'Alice à l'aide de la commande `tr` ?

Un beau soir, en rentrant du cours de yoga, Ève a trouvé un carnet rouge près de la maison de son voisin Bob. Ce carnet était rempli de mots étranges au premier regard... Ayant des connaissances dans la cryptographie, Ève a tout compris ! Ensuite, elle a mit le cahier dans la boîte aux lettres de Bob, en ajoutant le message suivant :

```
UV OBO, GUVF VF LBHE ARVTUOBE RIR. WHFG JNAAN FNL GUNG
EBG13 VF ABG IREL FGEBAT PVCURE.
```

EXERCICE 1.2. Écrivez un programme `inter-crypt.sh` qui chiffre (avec ROT13) de manière interactive les chaînes de caractères. Après le lancement du programme, l'utilisateur entre une chaîne de caractères et le programme répond avec une version cryptée

Exemple :

```
[user@machine /home/user/conversations]$ ./inter-crypt.sh
HELLO ← l'utilisateur entre une chaîne
URYYB ← logiciel lui répond

BOB ← l'utilisateur entre une autre chaîne
OBO ← logiciel lui répond

I'M ALICE ← l'utilisateur entre une autre chaîne
V'Z NYVPR ← logiciel lui répond
```

Indice : utilisez `while`, `read` et `tr`.

EXERCICE 1.3. Écrivez un programme `inter-decrypt.sh` qui déchiffre (avec ROT13) de manière interactive les chaînes de caractères.

Substitution monoalphabétique

Bob a dit à Alice qu'Éve était capable de déchiffrer leur correspondance. Le lendemain, Alice a croisé Bob á la cantine. Elle a dit à voix basse "c'est la clé" en lui donnant un morceau d'une serviette en papier sur lequel était écrit :

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
IJPYZQRSTUVWXABCKLMNODEFGH
```

Dans quelques jours, Bob a reçu une nouvelle lettre cryptée par l'algorithme de la substitution monoalphabétique :

```
ZDZ MZZXM NB JZ TANZWWTRZAN ZABORS NB YZPLGCN XG XZMMIRZM, XIGJZ EZ
MSBOWY TADTNZ SZL NB INNZAY BOL OAYZLRLBOAY OATF IAY PLGCNBRLICSG
PWIMMZM...  EBOWY GBO XTAY TQ T TADTNZ SZL NB UBTA OM AZFN NTXZ ?
```

EXERCICE 1.4. Déchiffrez ce message.

EXERCICE 1.5. Écrire deux scripts de Bash `crypt` et `decrypt` permettant de chiffrer et déchiffrer des fichiers à l'aide d'une clé.

Par exemple, afin de remplacer le fichier `file.txt` par un fichier `file.sumo` contenant la version cryptée du contenu du fichier `file.txt` en utilisant la clé contenant dans le fichier `clef.key`, l'utilisateur demande au système Unix :

```
./crypt file.txt clef.key
```

EXERCICE 1.6. En utilisant les redirections UNIX et nc transférez le fichier crypté d'un ordinateur à un autre.

EXERCICE 1.7. Décrypter le fichier sur un autre ordinateur.

```
./decrypt file.sumo clef.key
```

EXERCICE★ 1.8. Trouvez une méthode de décryptage des messages cryptés par l'algorithme de la substitution monoalphabétique si vous ne connaissez pas la clé.